6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 20

[GN Docket No. 13-111; FCC 17-25]

Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission seeks additional comment on a broad range of steps the Commission can take to help eliminate the problem of contraband wireless devices in correctional facilities. In particular, the Commission proposes a process for wireless providers to disable contraband wireless devices once they have been identified. The Commission seeks comment on additional methods and technologies that might prove successful in combating contraband device use in correctional facilities, and on various other proposals related to the authorization process for contraband interdiction systems and the deployment of these systems.

DATES: Interested parties may file comments on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments on or before **[INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by GN Docket No. 13-111, by any of the following methods:

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the Commission's Electronic Comment Filing System (ECFS): http://fjallfoss.fcc.gov/ecfs2/. See Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998).
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. Generally if more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking

number. Commenters are only required to file copies in GN Docket No. 13-111.

- Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
    - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
    - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

People with Disabilities: To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

FOR FURTHER INFORMATON CONTACT: Melissa Conway, Melissa.Conway@fcc.gov, of the Wireless Telecommunications Bureau, Mobility Division, (202) 418-2887. For additional information concerning the PRA information collection requirements contained in this document, contact Cathy Williams at (202) 418-2918 or send an email to PRA@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further Notice of Proposed Rulemaking (FNPRM) in GN Docket No. 13-111, FCC 17-25, released on March 24, 2017. The complete text of the FNPRM is available for viewing via the Commission's ECFS website by entering the docket number, GN Docket No. 13-111. The complete text of the FNPRM is also available for public inspection and copying from 8:00 a.m. to 4:30 p.m. Eastern Time (ET) Monday through Thursday or from 8:00 a.m. to 11:30 a.m. ET on Fridays in the FCC Reference Information Center, 445

12th Street S.W., Room CY-B402, Washington, DC 20554, telephone 202-488-5300, fax 202-488-5563.

This proceeding shall continue to be treated as a "permit-but-disclose" proceeding in accordance with the Commission's ex parte rules (47 CFR 1.1200 et seq.). Persons making ex parte presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral ex parte presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the ex parte presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during ex parte meetings are deemed to be written ex parte presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written ex parte presentations and memoranda summarizing oral ex parte presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules.

The Commission will send a copy of the FNPRM in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

I. FNPRM

1. The use of contraband wireless devices in correctional facilities to engage in criminal activity poses a significant and growing security challenge to correctional facility administrators, law enforcement authorities, and the general public.

2. As a general matter, there are primarily two categories of technological solutions currently deployed today in the U.S. to address the issue of contraband wireless device use in correctional facilities: managed access and detection. A managed access system (MAS) is a micro-cellular, private network that typically operates on spectrum already licensed to wireless providers offering commercial subscriber services in geographic areas that include a correctional facility. These systems analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized by the correctional facility for purposes of accessing wireless carrier networks. A MAS utilizes base stations that are optimized to capture all voice, text, and data communications within the system coverage area. When a wireless device attempts to connect to the network from within the coverage area of the MAS, the system cross-checks the identifying information of the device against a database that lists wireless devices authorized to operate in the coverage area. Authorized devices are allowed to communicate normally (i.e., transmit and receive voice, text, and data) with the commercial wireless network, while transmissions to or from unauthorized devices are terminated. A MAS is capable of being programmed not to interfere with 911 calls. The systems may also provide an alert to the user notifying the user that the device is unauthorized. A correctional facility or third party at a correctional facility may operate a MAS if authorized by the Commission, and this authorization has, to date, involved agreements with the wireless providers serving the geographic area within which the correctional facility is located, as well as spectrum leasing applications approved by the Commission.

3. Detection systems are used to detect devices within a correctional facility by locating, tracking, and identifying radio signals originating from a device. Traditionally, detection systems use passive, receive-only technologies that do not transmit radio signals and do not require separate Commission

authorization. However, detection systems have evolved with the capability of transmitting radio signals to not only locate a wireless devices, but also to obtain device identifying information. These types of advanced transmitting detection systems also operate on frequencies licensed to wireless providers and require separate Commission authorization, also typically through the filing of spectrum leasing applications reflecting wireless provider agreement.

4. The Commission has taken a variety of steps to facilitate the deployment of technologies by those seeking to combat the use of contraband wireless devices in correctional facilities, including authorizing spectrum leases between CMRS providers[1] and MAS providers and granting Experimental Special Temporary Authority (STA) for testing managed access technologies, and also through outreach and joint efforts with federal and state partners and industry to facilitate development of viable solutions. In addition, Commission staff has worked with stakeholder groups, including our federal agency partners, wireless providers, technology providers, and corrections agencies, to encourage the development of technological solutions to combat contraband wireless device use while avoiding interference with legitimate communications.

5. On May 1, 2013, the Commission issued the Notice of Proposed Rulemaking (NPRM) (78 FR 36469, June 18, 2013) in this proceeding in order to examine various technological solutions to the contraband problem and proposals to facilitate the deployment of these technologies. In the NPRM, the Commission proposed to require CMRS licensees to terminate service to detected contraband wireless devices within correctional facilities pursuant to a qualifying request from an authorized party and sought comment on any other proposals that would facilitate the deployment of traditional detection systems. Technology has evolved such that many advanced detection systems are designed to transmit

[1] Unless otherwise specifically clarified herein, for purposes of the FNPRM, we use the terms CMRS provider, wireless provider, and wireless carrier interchangeably. These terms typically refer to entities that offer and provide subscriber-based services to customers through Commission licenses held on commercial spectrum in geographic areas that might include correctional facilities.

radio signals typically already licensed to wireless providers in areas that include correctional facilities. Consequently, operators of these types of advanced detection systems require Commission authorization. Accordingly, we will refer to any system that transmits radio communication signals comprised of one or more stations used only in a correctional facility exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or to obtain identifying information from such contraband wireless devices as a Contraband Interdiction System (CIS).[2] By definition, therefore, the processes proposed in the FNPRM are limited to correctional facilities' use.

Disabling Contraband Wireless Devices in Correctional Facilities

6. In the NPRM, the Commission sought comment on each of the steps involved in the process of terminating service to contraband wireless devices, including the information that the correctional facility must transmit to the provider to effectuate termination, the timing for carrier termination, the method of authenticating a termination request, and other issues. CellAntenna has proposed a termination process that includes minimum standards for detection equipment, the form of notice to the carrier, and a carrier response process that consists of a set of deadlines for responding, based on the volume of reports or inquiries the carrier receives concerning contraband wireless devices. Under this staged response obligation, the carriers would have a longer time to respond if they receive a large number of requests, ranging from one hour to 24 hours after receipt of notice. CellAntenna encourages the Commission to determine a "reasonable" time frame for service suspension.

[2] For purposes of the FNPRM, "contraband wireless device" refers to any wireless device, including the physical hardware or part of a device – such as a subscriber identification module (SIM) – that is used within a correctional facility in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy. We use the phrase "correctional facility" to refer to any facility operated or overseen by federal, state, or local authorities that houses or holds criminally charged or convicted inmates for any period of time, including privately owned and operated correctional facilities that operate through contracts with federal, state, or local jurisdictions.

7. Commenting parties focused substantially on the issue of liability associated with termination, and their alternative proposal that termination should be required only pursuant to a court order. Wireless carriers expressed concern that the proposed termination process would require carriers to investigate requests and risk erroneous termination, which could endanger safety and create potential liability. Instead, the carriers argue, the Commission should amend its proposed termination rules to require that requests to terminate be executed pursuant to an order from a court of relevant jurisdiction. Other commenters, however, reject the notion that court-ordered termination is necessary in order to protect carriers from liability in the event of erroneous termination, and argue that the Commission's role in managing the public's use of spectrum empowers it to require carriers to terminate service to unlawful devices, irrespective of whether the request is made by the FCC, a court order, or upon the request of an authorized prison official.

8. We seek further comment on a Commission rule-based process regarding the disabling of contraband wireless devices where certain criteria are met, including a determination of system eligibility and a validation process for qualifying requests designed to address many wireless provider concerns. We clarify that a disabling process would involve participation by stakeholders to effectively implement a Commission directive to disable such devices, and would in no way represent a delegation of authority to others to compel such disabling. We recognize that wireless providers favor a court-ordered termination process as an alternative, but requiring court orders might be unnecessarily burdensome. Based on the comments filed in the record, moreover, it is far from clear that a CMRS provider that terminates service to a particular device based on a qualifying request would be exposed to any form of liability. Indeed, we welcome comment from CMRS providers on the scope of their existing authority under their contracts and terms of service with consumers to terminate service. Commenters who agree with the view that a court-ordered approach is preferable should specifically address why termination pursuant to a federal requirement, i.e., Commission directive, does not

address liability concerns as well as termination pursuant to court order. We note that the current record does not sufficiently demonstrate that reliance on the wireless providers' alternative court-ordered approach in lieu of the proposed rule-based approach discussed below would achieve one of the Commission's overall goals in this proceeding of facilitating a comprehensive, nationwide solution. We also note that the record does not reflect persuasive evidence of successful voluntary termination of service to contraband wireless devices in correctional facilities by the CMRS licensees, even where there is evidence of a growing problem.

9. To the extent commenters continue to support a court-ordered approach, we seek specific comment on the particulars of the requested court-ordered process to evaluate and compare it to a Commission disabling process: who is qualified to seek a court order and with what specific information or evidence? To whom is the request submitted and how is the court order implemented? How can existing processes carriers use for addressing law enforcement requests/subpoenas apply in the contraband wireless device context? Does the success of a court-ordered process depend on the extent to which a particular state has criminalized wireless device use in correctional facilities? Additionally, given the acknowledged nationwide scope and growth of the contraband wireless device problem, how would CIS and wireless providers navigate the myriad fora through which requests for termination might flow, potentially requiring engagement with a wide variety of state or federal district attorneys' offices; federal, state or county courts; or local magistrates? In this regard, we seek examples of successfully issued and implemented court orders terminating service to contraband wireless devices, as well as demonstrations that court orders can be effective at scale and not overly burdensome or time-consuming to obtain and effectuate in this context.

10. Commission Authority. In the NPRM, the Commission stated its belief that the Commission has authority under section 303 to require CMRS licensees to terminate service to contraband wireless devices. AT&T recognizes the Commission's authority pursuant to section 303 to require termination,

but argues that deactivation must be ordered by a court or the FCC because the Commission cannot lawfully delegate its statutory authority to a third party, such as a state corrections officer. In response, Boeing and Triple Dragon reject AT&T's position, arguing that the proposed termination process does not raise any issues of delegation, as the Commission has clear authority to require carriers to terminate service to unauthorized devices upon receiving a Commission-mandated qualifying request. Section 303 provides the Commission authority to adopt rules requiring CMRS carriers to disable contraband wireless devices (see 47 U.S.C. 303; see also 154(i)). Pursuant to section 303(b), the Commission is required to prescribe the nature of the service to be rendered by each class of licensed stations and each station within any class. Additionally, section 303(d) requires the Commission to determine the location of classes of stations or individual stations, and section 303(h) grants the Commission the authority to establish areas or zones to be served by any station. When tied together with section 303(r), which requires the Commission to make such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter, these provisions empower the Commission to address these issues.

11. Further, with respect to wireless carrier arguments that any proposal for requests by departments of corrections based on CIS-collected data seeking disabling of contraband wireless devices is an unlawful delegation of authority, we clarify that any such request would be pursuant to an adopted Commission rule mandating disabling where certain criteria are met. Such criteria, as discussed in detail below, include various factors involving the deployment of CIS technologies. The Commission's authority under section 303 to regulate the use of spectrum in the public interest necessarily includes the authority to promulgate rules requiring regulated entities to terminate unlawful use of spectrum where certain indicia are met. We seek comment on a process by which carriers would be required to disable contraband devices identified through CIS systems deemed eligible by the Commission. The

Commission would not be delegating decision-making authority regarding the disabling of contraband wireless devices.

12. Disabling of Contraband Wireless Devices in Correctional Facilities. We seek comment on a process whereby CMRS licensees would disable contraband wireless devices in correctional facilities detected by an eligible CIS when they receive a qualifying request from an authorized party. We seek comment on a range of issues, including CIS eligibility, what constitutes a qualifying request, and specifics regarding the carrier disabling process. We clarify that CIS systems operating solely to prevent calls and other communications from contraband wireless devices, described in the Notice as MASs, would not be subject to these eligibility criteria, unless the department of corrections/CIS provider seeks to use the information received from such a system to request, through Commission rules, contraband wireless device disabling.

13. Numerous individual state departments of corrections support the Commission's proposal to mandate termination of service to contraband wireless devices. For example, the Chief Information Officer of the Texas Department of Criminal Justice encourages implementation of a termination of service process, including criteria establishing a maximum allowable time limit for termination of service upon proper notification by an authorized correctional official. The Minnesota Department of Corrections supports a nationally standardized protocol for identifying contraband wireless devices and notification to the carrier. The Florida Department of Corrections also supports the standardization of information required to be provided by correctional facilities to service providers for termination of service and of the method of submission of information. The Mississippi Department of Corrections supports a Commission mandate to terminate service to contraband wireless devices, noting that it has made efforts to terminate service by seeking court orders with the cooperation of some wireless providers, that not all providers have been cooperative, and that a Commission rule would save time and resources used in obtaining a court order.

14. Several commenters express concern regarding the validation process and accuracy of termination information relayed to the carriers to implement termination of service to contraband wireless devices in correctional facilities. The carriers assert that the record simply does not contain sufficient information to define a process for termination at this time. AT&T suggests that there must be a validation process whereby carriers have the opportunity to confirm the accuracy of the termination information. AT&T is concerned that if there is not an FCC or court order compelling termination, the carrier bears the responsibility for deciding whether to terminate service to a particular device. Verizon also expresses significant concern regarding the dearth of carrier experience with handling termination requests. Verizon contends that carriers have material concerns regarding the ability of detection systems to accurately identify contraband devices, the security and authenticity of the termination requests being transmitted to carriers, and the potential liability of carriers for erroneous termination. Verizon believes that carriers require accurate information about the MIN and the device MDN,[3] and therefore the Commission should review and certify managed access and detection systems. Verizon also recommends that termination requests be transmitted via secure transmission paths such as secure web portals that already exist to receive court-ordered termination requests.

15. Furthermore, Verizon claims that, due to the lack of information in the record, it is impossible at this time to determine important details about termination requests, such as how many entities will be making such requests, how frequently those requests will be made, and how many devices carriers will be asked to terminate in each request. As a result, Verizon states, carriers have no way of assessing the costs of processing termination requests or the systems that will have to be in place. CTIA concurs that, in light of the complexities in the termination proposal, the Commission should certify detection systems

[3] MIN is the mobile identification number and MDN is the mobile directory number. The MIN and the MDN are used by CDMA devices.

and validate that a detection system is working properly and capturing accurate, necessary information regarding the unauthorized devices. One managed access provider, CellBlox, opposes proposals to require termination of service to contraband wireless devices not only as unworkable and burdensome to correctional facilities, but also as raising too many unanswered questions regarding the specifics of the termination process.

16. Tecore is a proponent of MASs as the preferred solution to the contraband problem, but is not opposed to detection and termination solutions used in conjunction with MAS, if the Commission establishes the specifics for a termination process. To the extent that the Commission decides to mandate termination procedures, Tecore implores the Commission to define specific information that the correctional facility must transmit to the carrier in order to effectuate a termination, including device information, criteria for concluding that a device is contraband, a defined interface for accepting or rejecting a request, a defined timeframe, and procedures for protesting or reinstating an invalid termination.

17. Triple Dragon supports Commission regulations governing the detection and termination of service to contraband wireless devices and urges the Commission to revise its rules to accommodate an equipment certification process for detection systems. With regard to the timeframe for carriers to terminate service subsequent to a request, Triple Dragon suggests that immediate termination is necessary for public safety and that termination should be based on clear data indicating that the device is operating in violation of federal or state law or prison policy. Boeing contends that performance standards or additional technical requirements for passive detection systems are unnecessary and impractical. Boeing highlights that, despite numerous and lengthy trials of detection technology at various facilities around the country, there have been no reports of misidentification. Indeed, Boeing believes that there is a lack of evidence to warrant the imposition of technical requirements for

detection systems, noting that the record does not show an appreciable risk of misidentification, nor does it support the imposition of burdensome technical standards to address this hypothetical risk.

18. Other stakeholders encourage the Commission to foster the development of all solutions to combat contraband wireless devices in correctional facilities, including detection and termination. The supporters of termination include providers of inmate calling services. Securus recommends that the Commission should not preclude any of these alternatives and should support the testing and implementation of all these options. Further, Securus suggests that the FCC should take a firm stance that CMRS providers must cooperate with correctional facilities to quickly terminate service to detected contraband devices. GTL supports the Commission's proposal to require wireless carriers to terminate service to contraband wireless devices, without the need for a court order. GEO, a private manager and operator of correctional facilities, agrees with the Commission's proposal to require carriers to terminate service to contraband wireless devices within one hour of receipt of notice from a qualifying authority. GEO recommends a broad definition of qualifying authority that would include wardens of both private and public correctional facilities. ACA urges the Commission to permit the corrections community to employ every possible tool in the toolbox to combat contraband wireless devices in correctional facilities, including immediate termination of service by carriers upon notification by any public safety agency pursuant to a standardized process. Acknowledging the carriers' concern about potential liability for erroneous termination, ACA suggests that the Commission adopt rules granting carriers protection while acting in good faith and for public safety to further protect the carriers above and beyond the language in the customer contracts.

19. After careful consideration of the record, we seek further comment on a process whereby CMRS licensees would disable contraband wireless devices in correctional facilities detected by an eligible CIS pursuant to a qualifying request that includes, inter alia, specific identifying information regarding the device and the correctional facility. We seek to ensure that any disabling process will completely disable

the contraband device itself and render it unusable, not simply terminate service to the device as the Commission had originally proposed in the NPRM. We seek comment on whether a process should include a required FCC determination of eligibility of CISs to ensure the systems satisfy minimum performance standards, appropriate means of requesting the disabling, and specifics regarding the required carrier response. We seek specific comment on all aspects of the process as well as the costs and benefits of their implementation.

20. Eligibility of CISs. We seek to ensure that the systems detecting contraband wireless devices first meet certain minimum performance standards in order to minimize the risk of disabling a non-contraband wireless device. We therefore seek comment on whether it is necessary to determine in advance whether a CIS meets the threshold for eligibility to be the basis for a subsequent qualifying request for device disabling, which might facilitate contracts between stakeholders, for example departments of corrections and CIS providers, and appropriate spectrum leasing arrangements, typically between CIS providers and wireless providers. We envision that any eligibility determination would not at this stage assess the CIS's characteristics related to a specific deployment at a certain correctional facility, but rather a CIS's overall methodology for system design and data analysis that could be included in a qualifying request, where more specific requirements must be met for device disabling. We seek comment on whether a CIS operator seeking wireless provider disabling of contraband wireless devices in a correctional facility should first be deemed an eligible CIS by the Commission, and whether the Commission should periodically issue public notices listing all eligible CISs. We seek comment on the following potential criteria for determining eligibility: (1) all radio transmitters used as part of the CIS have appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility,[4] can secure and protect the collected

[4] To comply with this criteria, a CIS operator may need to employ a range of mitigation techniques that might vary depending on the location of the correctional facility, as rural v. urban facilities differ substantially regarding their proximity to the general public.

information, and is capable of being programmed not to interfere with emergency 911 calls; and (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to provide a high degree of certainty that the particular wireless device subject to a later disabling request is in fact located within a correctional facility. We also seek comment on the appropriate format for requesting eligibility, taking into consideration our goal of reducing burdens and increasing administrative efficiency.

21. We seek further comment on the costs, benefits, and burdens to potential stakeholders of requiring CIS eligibility before qualifying disabling requests can be made to wireless providers and whether the stated eligibility criteria adequately address concerns expressed in the record regarding improper functioning of CIS systems and inaccurately identifying contraband devices. If commenters disagree, we seek comment on what additional eligibility criteria would ensure the accuracy and authenticity of CISs. For example, should we require testing or demonstrations at a specific correctional facility prior to making a CIS eligibility determination? If so, what type of tests would be appropriate? How should signals be measured and what criteria should be used to evaluate such tests? Importantly, should such a testing requirement be part of the initial eligibility assessment or should it part of what constitutes a qualifying request? If testing were part of a general eligibility assessment, would such additional testing at a specific site be unduly burdensome or unnecessarily delay or undermine either state RFP processes or spectrum lease negotiations? Would parties enter into agreements and lease arrangements where a CIS had not yet been deemed eligible? Should we require that a CIS be able to identify the location of a wireless device to within a certain distance? Is such an accuracy requirement unnecessary or would it be beneficial in assessing the merits of a CIS design and reducing the risk of capturing non-contraband devices? Should any eligibility determination be subject to a temporal component, for example, requiring a representation on an annual basis that the basic system design and data analysis methodology have not materially changed, and should the CIS operator be required to

provide the Commission with periodic updates on substantial system changes, upgrades, or redesign of location technology? Should eligibility be contingent on the submission of periodic reports detailing any incidents during the applicable period where devices were erroneously disabled? Should the eligibility criteria be different depending on whether the facility is in a rural or urban area, or whether the CIS provider, the correctional facility, or the CMRS licensee is large or small? Commenters should be specific in justifying any proposed additional minimum standards for CIS eligibility, including the costs and benefits to stakeholders.

22. Qualifying Request. In addition to ensuring that CISs meet certain performance standards in order to minimize the risk of error, we also seek to ensure that an authorized party provides the information necessary for a wireless provider to disable contraband wireless devices. We seek comment on potentially requiring CMRS licensees to comply with a disabling process upon receipt of a qualifying request made in writing and transmitted via a verifiable transmission mechanism.[5] We seek comment on whether the qualifying request must be transmitted (1) by the Commission (including, potentially, by the contraband wireless device ombudsperson referenced above), upon the request of a Designated Correctional Facility Official (DCFO); or (2) by the DCFO. We seek comment on whether we should define the DCFO as a state or local official responsible for the facility where the contraband device is located. We seek specific comment on the costs and benefits of these two approaches to the transmission of the qualifying request, both in terms of timeliness and any perceived liability concerns.

23. We seek comment on whether carrier concerns about the authenticity of termination requests are best addressed by requiring that a request to disable be initiated by a state or local official responsible for the correctional facility, who arguably has more responsibility and oversight in the procurement of a CIS for correctional facilities than a warden or other prison official or employee, as

[5] A verifiable transmission mechanism is a reliable electronic means of communicating a disabling requesting that will provide certainty regarding the identity of both the sending and receiving parties.

suggested in the record. A review of our ULS and OET databases reflects that, to date, requests for Commission authorization of CISs have only been in state correctional facilities, but we seek to facilitate a wide range of deployments where possible to achieve a more nationwide solution, including within federal and/or local correctional facilities that may seek to deploy CIS. We also seek specific comment on the extent to which, as Verizon claims, carriers have existing secure electronic means used to receive court-ordered termination requests, which could be leveraged to transmit and receive disabling requests from correctional facilities that employ CISs.

24. We seek comment on whether a qualifying disabling request should include a number of certifications by the DCFO, as well as device and correctional facility information. Should the DCFO certify in the qualifying request that (1) an eligible CIS was used in the correctional facility, and include evidence of such eligibility; (2) the CIS is authorized for operation through a license or Commission approved lease agreement, referencing the applicable ULS identifying information; (3) the DCFO has contacted all CMRS licensees providing service in the area of the correctional facility for which it will seek device disabling in order to establish a verifiable transmission mechanism for making qualifying requests and for receiving notifications from the licensee; and (4) it has substantial evidence that the contraband wireless device was used in the correctional facility, and that such use was observed within the 30 day period immediately prior to the date of submitting the request? We seek comment on this process and any methods in which the Commission can facilitate interaction between the authorized party and the CMRS licensees during the design, deployment, and testing of CISs. For example, would it be useful for the Commission to maintain a list of DCFOs? What role could the contraband ombudsperson play in facilitating the interaction between DCFOs and CMRS licensees?

25. Finally, we seek comment on whether a qualifying request should include specific identifying information regarding the device and the correctional facility. Should the request include device identifiers sufficient to uniquely describe the device in question and the licensee providing CMRS service

to the device? We seek comment on whether including the CMRS licensee is warranted if the request is made directly to the Commission, but unnecessary if the request is made directly from a DCFO to the CMRS licensee able to confirm that the device is a subscriber on its network. With regard to device identifiers, we seek specific comment on whether other details are necessary in addition to identifiers that uniquely describe the specific devices, such as make and model of the device or the mode of device utilization at the time of detection. Is it relevant whether the device – at the time of detection – was making an incoming or outgoing voice call, incoming or outgoing SMS text or MMS (multimedia) message, or downloading or uploading data?

26. We seek additional comment on whether other details are necessary in terms of location and time identifiers, such as latitude and longitude to the nearest tenth of a second, or frequency band(s) of usage during the detection period, in order to accurately identify and disable the device. Is it necessary to require that a request include specific identifiers to accurately identify and disable the device, or would providing the flexibility to include alternative information to accommodate changes in technology be appropriate, and what types of alternative information would further our goal of an efficient disabling process? Specifically, what is necessary to accurately identify and disable the device? For example, common mobile identifiers include international mobile equipment identifier (IMEI) and the international mobile subscriber identity (IMSI), used by GSM, UMTS, and LTE devices; and electronic serial number (ESN), mobile identification number (MIN), and mobile directory number (MDN), used by CDMA devices. Should additional information be required to accurately identify a specific wireless device for requested disabling? Are there significant differences in the identifying information of current wireless devices (e.g., android, iOS, windows) that must be accounted for? We seek to minimize burdens for those providing information, by only requiring what is essential to properly disable.

27. We seek comment on whether there are commonalities that would permit standardized information sharing, while still taking into account the full range of devices, operating systems, and

carriers. We also seek comment on the appropriate format of a qualifying request to streamline the process and reduce administrative burdens. Would it be more efficient for carriers to develop a common data format so that corrections facilities, through a DCFO, are not required to develop a different format for each wireless provider? Should any of these possible requirements vary depending on whether the wireless provider is small or large?

28. In comments, Tecore raises the concern that SIM cards can be easily replaced so that devices are only temporarily deactivated. The record indicates that termination of service alone may be an incomplete solution capable of inmate exploitation. We therefore seek comment on a potentially more effective approach to ensure that not only is service terminated to the detected contraband device, but also that the device is rendered unusable on that carrier's network. We seek comment on the technical feasibility of a disabling process, including the costs and benefits of implementation, as well as any impact on 911 calls. We note that a disabled device will not have 911 calling capability, whereas a service terminated device would maintain 911 calling capability pursuant to the Commission's current rules regarding non-service initialized (NSI) phones.[6] Should we maintain the requirement that CMRS carriers keep 911 capability for disabled contraband phones, subject to the outcome of the NSI proceeding? What are the costs and benefits to stakeholders of such a requirement?

29. We seek comment on whether a qualifying request should also include correctional facility identifiers, including the name of the correctional facility, the street address of the correctional facility, the latitude and longitude coordinates sufficient to describe the boundaries of the correctional facility, and the call signs of the Commission licenses and/or leases authorizing the CIS. Would this information provide sufficiently accurate information about the correctional facility to ensure that the carrier can restrict the disabling of wireless devices to those that are located within that facility?

[6] The Commission has proposed revising its rules to sunset, after a six month period, the requirement that NSI phones be 911 capable.

30. Disabling Process. As a preliminary matter, we seek to ensure that such requests can be transmitted in an expeditious manner and to have confidence that the request will be received and acted upon. Should the CMRS licensee be required to provide a point of contact suitable for receiving qualifying requests to disable contraband wireless devices in correctional facilities? We also recognize the need to safeguard legitimate devices from being disabled. Accordingly, we seek comment on what steps, if any, the CMRS licensee should take to verify the information received, whether customer outreach should be part of the process, and the time frame within which the steps must be taken. We seek information to assist us in determining what level of carrier investigation, if any, is warranted to determine whether there is clear evidence that the device sought to be disabled is not contraband. We also seek comment on what level of customer outreach, if any, would ensure that the disabling request is not erroneous.

31. With regard to customer outreach, we again seek comment on a range of approaches, including the carrier immediately disabling without any customer outreach, the carrier contacting the subscriber of record through any available means (e.g., text, phone, email) and providing a reasonable amount of time prior to disabling for the customer to demonstrate that the disabling request is in error. We seek comment on whether a particular alternative enables inmates to evade device disabling. Each of these approaches impacts carrier response time and the ability to address, however unlikely, disabling errors. If some level of carrier investigation or customer outreach is warranted, should we provide CMRS licensees a method to reject a qualifying request if it is determined the wireless device in question is not contraband?

32. We seek comment on whether the CMRS licensee should provide notification to the DCFO within a reasonable time period that it has either disabled the device or rejected the request. We seek comment on what the reasonable time period should be for this notification, whether the licensee must provide an explanation for the rejection, and whether the DCFO can contest the rejection. We seek

comment on all aspects of a disabling process regarding verification of disabling requests, particularly the costs and benefits to the wireless providers, CIS operators, and the correctional facilities.

33. Timeframe for Disabling. We seek comment on various options for the appropriate timeframe for disabling a contraband wireless device, or rejecting the request if appropriate, each of which might be impacted by the range of potential levels of carrier investigation in independently verifying a disabling request and engaging in customer outreach. CellAntenna recommends a staged obligation between one hour and 24 hours depending on the volume of requests, and other commenters suggest immediate action or action within one hour. These positions would be consistent with CMRS licensees disabling devices without any independent investigation or, at best, after a brief period of research using readily available resources, but achieve the goal of promptly disabling contraband wireless devices. In contrast, if carriers disable devices following exhaustive research or customer outreach, a period of seven days or more would likely be more appropriate. While providing greater assurance that the disabling is not an error, a longer period allows further use of an identified contraband phone.

34. If the carrier attempts to contact the device's subscriber of record to permit a legitimate user the opportunity to demonstrate that the device is not contraband, how long should the user have to respond and does this notification requirement unnecessarily prolong device disabling? To what extent could a longer notification period increase the risk of inadvertently tipping off the user of a contraband device and thereby create opportunities for malefactors to cause harm or circumvent the correctional facility's efforts to address the illegal use? We seek specific comment regarding what periods of time are required in order to adequately balance the public safety needs with wireless provider concerns. We also seek comment on whether small entities face any special or unique issues with respect to disabling devices such that they would require additional time to comply.

35. Finally, we seek comment on the methods available to ensure that any process for determining CIS eligibility minimizes the risk of disabling customers' devices that are not located within correctional facilities, and any related costs and benefits. Are there contractual provisions in existing contracts between CMRS providers and their customers that address this or similar issues? We seek comment on what period of time would be reasonable to expect a CMRS licensee to reactivate a disabled device. For example, what methods of discovery will sufficiently confirm that a wireless device is not contraband? Is 24 hours a reasonable period to resolve potential errors and how extensive is the burden on subscribers to remain disabled for that period? What is the most efficient method of notifying the carriers of errors, if originating from parties outside a correctional facility, and of notifying subscribers of reactivation?

36. In the NPRM, the Commission also sought comment on CellAntenna's proposal that we adopt a rule to insulate carriers from any legal liability for wrongful termination, while noting that wireless carriers' current end user licensing agreements may already protect the carriers. We seek further comment on this proposal. Specifically, we seek comment on whether the Commission should create a safe harbor by rule for wireless providers that comply with the federal process for disabling phones in correctional facilities. How broadly should that safe harbor be written, and should it apply only to wireless providers that comply with every aspect of the rules we adopt or also those that act in good-faith to carry out the disablement process? Does the Commission have authority to adopt a safe harbor? Is our authority to adopt the rules at issue sufficient to create a safe harbor? Are there other provisions of the Communications Act not previously discussed that would authorize a safe harbor? And what, if any, downsides are there to creating a safe harbor for wireless providers that comply with federal law?

37. In the NPRM, the Commission also sought comment on the extent to which providers or operators of managed access or detection systems comply with section 705 if they divulge or publish the

existence of a communication for the purpose of operating the system, and whether such providers or operators are entitled to receive communications under section 705. Section 705 of the Act generally prohibits, except as authorized under Chapter 119, Title 18 of the U.S. Code, any person "receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio" from divulging or publishing the "existence, contents, substance, purport, effect or meaning thereof" to another person other than through authorized channels (47 U.S.C. 605(a)). Additionally, Chapter 206, Title 18 of the U.S. Code, generally prohibits the use of pen register and trap and trace devices without a court order, subject to several exceptions including where a provider of a communications service obtains the consent of the user (18 U.S.C. 3121-3127). The Commission sought comment on whether any of the proposals regarding detection and MASs would implicate the pen register and trap and trace devices chapter of Title 18 of the U.S. Code.

38. ShawnTech believes that the operation of its MASs is in compliance with federal and state law concerning the use of pen register and trap and trace devices, but expresses concern that detection systems that function to terminate service to contraband devices may not be in compliance. In addition to the questions the Commission asked in the NPRM, we seek comment on whether and to what extent a system used to request wireless provider disabling of a contraband wireless device pursuant to a Commission rule raises issues under Title 18 or section 705 that may be different from those raised by MAS implementation.

39. Some commenters in response to the NPRM also have raised concerns about the applicability of the privacy obligations under section 222 of the Communications Act (47 U.S.C. 222). After review of the record, we do not find that comments submitted in response to the NPRM demonstrate that section 222 would prohibit a carrier from complying with a Commission rule mandating a disabling process. To the extent commenters maintain a contrary view, we seek comment on this issue clearly providing support for such a position and on any other relationship of section 222 to the FNPRM.

Notification to CIS Operators of Carrier Technical Changes

40. In the NPRM, the Commission sought comment generally on proposals submitted by interested parties regarding rule changes intended to expedite the deployment of MASs, including GTL's proposal to impose network upgrade notification obligations on carriers. In its original petition, GTL requested that the Commission adopt rules that require CMRS providers to notify MAS operators or prison administrators in advance of any network changes likely to impact the MAS and negotiate in good faith on the implementation timing of the change. The reason for the requirement, GTL explained, is that rapid technological evolution impacts the effectiveness of a MAS and could render them ineffective; for example, network changes such as changing power levels or antenna patterns could impact proper operation of the system. In its comments, ACA supports this notification requirement.

41. In its comments, MSS suggests that effective implementation of MAS requires mandatory coordination of network changes with the MAS operator. As an example, MSS cites the impact of a technical change such as a switch from 3G to 4G at a given base station for a given band. At the same time, MSS notes the possibility that carriers may find the coordination of network changes with MAS operators burdensome. Tecore has highlighted the importance of communicating with the carriers regarding changes in technologies and the need to modify MAS deployments to respond to those changes, which occur frequently. GTL has also reiterated the challenges it faces in keeping pace with the software changes required to respond to rapidly changing wireless technology. GTL suggests that policies must ensure that wireless carriers are active participants in the effort to eliminate contraband cellphone use.

42. We acknowledge that the effectiveness of CIS systems depends on coordination between CMRS licensees, CIS operators, and correctional facilities, yet we recognize that any carrier notification requirement must not be overly burdensome or costly or have a negative impact on consumers. T-

Mobile claims that the record on this issue is in need of further development, and that a notification requirement could impede carrier network management flexibility and could delay the rollout of new technologies which would negatively impact consumers and carriers.

43. We recognize that a notification requirement that is too broad in scope, resulting in the need to send notifications possibly on a daily basis for minor technical changes, could be unduly burdensome on CMRS licensees. We also recognize that lack of notice to CIS operators of certain types of carrier system changes could potentially result in the CIS not providing the strongest signal in the correctional facility, compromising the system's effectiveness if contraband communications pass directly to the carrier network. Accordingly, in the FNPRM, we seek comment on the appropriate scope of a notification requirement. Would it be appropriate to require CMRS licensees that are parties to lease arrangements for CISs in correctional facilities to provide written notification to the CIS operator in advance of adding new frequency band(s) to their service offerings or deploying a new air interface technology (e.g., a carrier that previously offered CDMA technology deploying LTE) so that CISs can be timely upgraded to prevent spectrum gaps in the system that could be exploited by users of contraband wireless devices? To what extent should we require notification for additional types of carrier network changes, as GTL proposed, and if so, what specific network changes (e.g., transmitter power or antenna modifications) should be included? We seek specific comment on what other carrier network changes implemented without notice to CIS providers could render the systems in the correctional facilities ineffective, while also seeking comment on whether it is unduly burdensome to require notification for every routine carrier network modification. Would it be feasible to adopt a rule requiring a CMRS licensee providing service at a correctional facility to notify a CIS provider in advance of any network change likely to impact the CIS? We seek comment on AT&T's position that CIS providers should be required to respond within 24 hours to any notification from a CMRS licensee that the CIS is causing adverse effects to the carrier's network.

44. We also seek comment on how far in advance the notification should be sent from the CMRS licensee to the CIS operator in order to allow for sufficient time to upgrade the CIS and enable continuous successful CIS operation with no spectrum gaps. Is a 90 day advance notification requirement reasonable? Would a 30 day advance notification requirement allow sufficient time for upgrades? Finally, we seek comment on whether and to what extent CMRS licensees are currently coordinating with CIS operators in this regard. For example, T-Mobile states that a notification requirement will not provide any benefit and is unnecessary because CIS providers conduct spectrum scans as part of daily operations to detect new bands and technologies and air interfaces in use and already coordinate this scanning with CMRS licensees. We seek comment on the costs and benefits of any suggested notification requirements.

Other Technological Solutions

45. In the NPRM, the Commission invited comment on other technological solutions to address the problem of contraband wireless devices in correctional facilities, including those solutions discussed in previously filed documents referred to in the NPRM.

46. "Quiet Zones." In response to the NPRM seeking comment regarding alternative technological solutions to the contraband problem, some commenters suggest that the Commission mandate "dead zones" or "quiet zones" in and around correctional facilities. Although the proposals vary somewhat from a technical perspective and are referred to by different names, the common goal seems to be the creation of areas in which communications are not authorized such that contraband wireless devices in correctional facilities would not receive service from a wireless provider.

47. CellAntenna's position is that the Commission has authority to modify spectrum licenses to create areas, such as in correctional facilities, in which wireless services are not authorized. CellAntenna refers to NTCH's recommendation for "quiet zones" where no licensee would be authorized to provide

services. CellAntenna suggests that, given the variability in geography, each local correctional facility should be allowed to determine its need for a "no service" zone and petition the Commission to establish the "no service" zone and procedures for the registration of complaints of interference outside of the zones. Despite the fact that CellAntenna references NTCH's comments, NTCH's plan for the designation of "quiet zones" similar to radio astronomy or other research facilities to cover correctional facilities appears to differ from CellAntenna's "no service" zones because, according to NTCH's plan, there would be an official entity responsible for preventing unauthorized communications and for offering service over authorized frequencies in the prison area, called the "Prison Service Provider." NCIC suggests that the Commission create "dead zones" around correctional facilities in which carriers would be required to prevent the signal from reaching the correctional facility. GTL agrees that the Commission should explore the creation of "dead zones" or "quiet zones."

48. Similar to a "no service" zone, MSS proposes an alternative approach called geolocation-based denial (GBD) which permits a correctional facility to request that the Commission declare the facility outside the service area of all CMRS carriers if the facility has at least 300 meters of space in all directions between secure areas accessible by inmates and areas with unrestricted public access. MSS describes GBD as a low-risk solution that will address highly problematic rural maximum security prisons. ACA supports the creation of "quiet zones" and GBD.

49. The carriers oppose the "quiet zone"-like proposals. AT&T opposes NCIC's proposal to create "quiet zones" around correctional facilities in which carriers are unauthorized to provide wireless service, claiming that a quiet zone would prevent the completion of legitimate emergency calls from the correctional facility and vicinity within the quiet zone. Even in rural areas, Verizon suggests, legitimate communications in the areas around prisons could be impacted. In opposing the idea of a quiet or exclusion zone, Verizon argues that these proposals would indiscriminately prevent legitimate communications, including public safety communications from being completed both inside and outside

the prison grounds. CTIA opposes the establishment of quiet zones because they would unnecessarily complicate wireless network design and be an intrusion on licensees' exclusive spectrum rights.

50. In the FNPRM, we seek additional comment on the proposals in the record for the mandatory creation of "quiet zones" or "no service" zones in order to help us better understand the similarities and differences among the proposals and receive more detailed information in the record regarding how the zones would be created from a legal and technical perspective. What are the methods wireless providers would use to create the quiet zone, including technical criteria used to define the zone? Should there be a field strength limit on the perimeter of the zone and, if so, what is the appropriate limit? Would the limits set forth in Commission rule 15.109 (47 CFR 15.109) applicable to unintentional radiators be appropriate and how would this be measured? Or would a different criterion, such as 15 dBu, be appropriate to ensure calls outside the perimeter could be completed while not providing the ability for connection to the network inside the perimeter? How would such a limit impact carrier network design? Again, we request that commenters elaborate on the role of the Commission in the creation of these zones and the legal basis for their establishment. We query whether "quiet zones" could be created voluntarily or whether there is a legal bar to their creation in the absence of Commission action. We also seek comment on the application of "geo-fencing" in the contraband wireless device context and how it differs from a "quiet zone." Just as geo-fencing software can prevent drones from flying over a specific location, could geo-fencing be used to create a virtual perimeter around a correctional facility such that wireless devices would be disabled within the geo-fence? We seek comment on whether geo-fencing could be used to create zones within which contraband wireless devices would be inoperable and whether this technology would permit the delivery of emergency calls within the zone or interfere with other legitimate communications outside the geo-fence.

51. Network-Based Solution. Relatedly, we seek comment on the concept of requiring CMRS licensees to identify and disable contraband wireless devices in correctional facilities using their own

network elements, including base stations and handsets/devices. As technology evolves, CMRS licensees are acquiring new and better ways of more accurately determining the precise location of a wireless device. Indeed, the Commission addressed the technological advances and need to improve location accuracy in the context of emergency 911 calling when it adopted E911 location accuracy deadlines aimed at enhancing PSAPs' ability to accurately identify the location of wireless 911 callers when indoors. In order to meet the Commission's requirements over the next several years, carriers will be required to deploy technology capable of locating wireless devices to within certain distances or coordinates. We also know that carriers currently have ways of determining the location of a wireless device using an analysis of call records or Global Positioning System (GPS) technology. In fact, more than 20 states have enacted legislation based on the Kelsey Smith Act (H.R. 4889, 114th Cong., 2d Sess. (2016)) that requires carriers to give law enforcement call location information in an emergency involving the risk of death or serious injury. Further, there are device applications (e.g., Uber or Google Maps) that enable the identification of the location of the device through GPS technology located in the device. Given the improved and evolving capability of carriers to identify the location of wireless devices, we seek comment on whether existing methodologies could also be effective in the context of contraband wireless devices in correctional facilities. We acknowledge that an approach relying solely on GPS technology may not be effective inside correctional facilities if the GPS capability can be disabled or if GPS signals are insufficient within the correctional facility. Further, we note that a carrier's ability to identify the location based on network (not device GPS) data is affected by the number, location, and orientation of carrier base stations in the area. That said, we seek comment on whether it is possible for CMRS licensees to use their own network elements to determine that a wireless device is in a correctional facility, and what are the costs and benefits of such a process.

52. If we require CMRS licensees to identify wireless devices in correctional facilities using their own network elements, should we require carriers to recognize whether contraband wireless devices are

persistently used in a correctional facility located in the carrier's geographic service area and to disable them using their own resources? How should we define "persistently"? How would the carriers determine that a wireless device in a correctional facility is, in fact, contraband? Should the carriers be required to have an internal process in place whereby they could reactivate a device disabled in error? If a network-based solution is feasible, should we require it only if a particular correctional facility requests this approach as opposed to the solution of requiring CMRS licensees to disable devices pursuant to qualifying requests as described above? Do particular types of wireless devices or carrier air interfaces present unique challenges? We seek comment on the implementation, technical, and other issues associated with this carrier network-based solution as well as the costs and benefits associated with this potential solution. In particular, what would the costs be to carriers of complying with a mandate of having to locate contraband wireless devices in all correctional facilities nationwide? Finally, we seek comment on whether the network-based solution described herein raises any privacy concerns, including the privacy obligations under section 222 of the Communications Act.

53. Beacon Technology. We also seek comment on technologies that are intended to disable contraband wireless devices in correctional facilities using the interaction of a beacon system set up in the correctional facility with software embedded in the wireless devices. Essentially, these types of technologies rely on a system of beacons creating a restricted zone in a correctional facility, such that any wireless device in the zone will not operate. One of the benefits of this approach is that this technology would appear to render the phone unusable by an inmate for any purpose. In other words, some of the technologies discussed above could prevent an inmate from placing a call, but they may not prevent the inmate from using the phone for taking videos or otherwise sharing or disseminating information that itself could pose a threat to public safety. We thus also seek comment on whether this type of technology—or elements thereof—can and should be incorporated into any other approach the Commission may take. For example, should we consider requiring that phones be rendered completely

unusable as part of our implementation of another solution, including the network-based solution discussed above.

54. At the same time, it appears that beacon-based technologies would function effectively only if all wireless carriers perform a system update to include the software for all existing and future wireless devices, and all mobile device manufacturers include the software in all devices. We seek comment on this technological solution, including costs and benefits of its implementation. Would this solution require legislation to ensure that all wireless carriers and wireless device manufacturers include the software in the wireless devices? In the absence of legislation, how would the Commission ensure wireless carrier and device manufacturer cooperation and pursuant to what authority would the Commission be acting? How would compliance be enforced? Should it be incorporated as part of the Commission's equipment certification requirements or be made part of an industry certification process? Would a "system update" actually accomplish the goal of ensuring that all wireless devices currently in existence get updated with the software? Would the beacon system in the correctional facility permit 911 or E911 calls from the restricted zone to be connected? Is a voluntary solution possible between the carriers and the providers of beacon technology?

55. We welcome comment on any other new technologies designed to combat the problem of contraband wireless devices in correctional facilities and what regulatory steps the Commission could take to assist in the development and deployment of these new technologies. We seek comment on what additional steps the Commission could take to address the contraband cellphone problem, for example, educational efforts designed to highlight available solutions, other expertise, or additional ways in which we can coordinate stakeholder efforts.

II. PROCEDURAL MATTERS

Initial Paperwork Reduction Act Analysis

56. The FNPRM contains proposed new information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by PRA. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how it might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

Initial Regulatory Flexibility Act Analysis

57. As required by the Regulatory Flexibility Act of 1980 (5 U.S.C. 603), the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules proposed in this document. We request written public comment on the IRFA. Comments must be filed in accordance with the same deadlines as comments filed in response to the FNPRM as set forth on the first page of this document, and have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the FNPRM, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration.

58. Need for, and Objectives of, the Proposed Rules. The FNPRM seeks comment on methods to provide additional tools to combat contraband wireless devices in correctional facilities. It is clear that inmate possession of wireless devices is a serious threat to the safety and welfare of correctional facility employees and the general public. First, as a safeguard to ensure coordination between CMRS licensees and CIS operators, the Commission seeks comment on a requirement that CMRS licensees that are parties to lease arrangements for CIS in correctional facilities provide written notification to the CIS operator no later than 90 days in advance of adding new frequency band(s) to its service offerings or deploying a new air interface technology (e.g., a carrier that previously offered CDMA deploying LTE), unless a different timeframe is agreed to by both parties. The Commission seeks comment on the

appropriate timing, costs, and alternatives to such a notice requirement. The FNPRM seeks comments on the types of notice protocol CMRS licensees might already have in place, and whether and how those procedures could be used to satisfy any notice requirement.

59. The FNPRM seeks comment on a requirement that CMRS providers disable a contraband wireless devices found by a CIS to be in correctional facilities pursuant to a qualifying request from an authorized party. The FNPRM seeks comment on a process that would include a CIS eligibility determination to ensure the systems satisfy minimum performance standards, appropriate means of requesting the disabling, and specifics regarding the required carrier response. The Commission seeks comment on maintaining a public list of all eligible CISs to facilitate expeditious lease transactions for those seeking to deploy systems resulting in requests for contraband wireless device disabling. We seek comment on the following criteria for determining eligibility: (1) the CIS has appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility, secure and protect the collected information, and avoid interfering with emergency 911 calls; and (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to provide a high degree of certainty that the particular wireless device is in fact located within a correctional facility. The Commission also seeks comment on these standards, and whether additional standards may be required for accuracy

60. To ensure that an authorized party provides the information necessary for a wireless provider to disable the contraband wireless devices, the Commission seeks comment on a requirement that CMRS licensees comply with a disabling process upon receipt of a qualifying request made in writing and transmitted via a verifiable transmission mechanism. The Commission seeks comment on whether the qualifying request must be transmitted (1) by the Commission upon the request of a Designated Correctional Facility Official (DCFO); or (2) by the DCFO. We seek comment on whether we should define the DCFO as a state or local official responsible for the facility where the contraband device is

located. In order for the request to disable a contraband device to be a qualifying request, the Commission also seeks comment on a requirement that the DCFO certify in the qualifying request that: (1) an eligible CIS was used in the correctional facility, and include evidence of such eligibility; (2) the CIS is authorized for operation through a license or Commission approved lease agreement, referencing the applicable ULS identifying information; (3) the DCFO has contacted all CMRS licensees providing service in the area of the correctional facility for which it will seek device disabling in order to establish a verifiable transmission mechanism for making qualifying requests and for receiving notifications from the licensee; and (4) it has substantial evidence that the contraband wireless device was used in the correctional facility, and that such use was observed within the 30 day period immediately prior to the date of submitting the request. The Commission seeks comment on these requirements and any methods to facilitate interaction between the authorized party and the CMRS licensees during design, deployment, and testing of CISs.

61. In the FNPRM, the Commission seeks comment on whether a qualifying request should include specific identifying information regarding the device and the correctional facility. Importantly, the Commission asks whether the request should include device identifiers sufficient to uniquely describe the device in question and the licensee providing CMRS service to the device. With regard to device identifiers, the Commission seeks specific comment on whether other details are necessary in addition to identifiers that uniquely describe the specific devices, such as make and model of the device or the mode of device utilization at the time of detection. The FNPRM also seeks comment on whether a qualifying request should also include correctional facility identifiers, including the name of the correctional facility, the street address of the correctional facility, the latitude and longitude coordinates sufficient to describe the boundaries of the correctional facility, and the call signs of the Commission licenses and/or leases authorizing the CIS.

62. In considering a process whereby CMRS licensees disable contraband wireless devices upon receiving a qualifying request, the Commission recognizes the need to safeguard legitimate devices from being disabled to the greatest extent possible. Accordingly, the FNPRM seeks comment on the appropriate steps, if any, the CMRS licensee should take to verify the information received, whether customer outreach should be part of the process, and the time frame within which the steps must be taken. The Commission seeks comment on a requirement that, if the DCFO is the authorized party transmitting the qualifying request to the CMRS licensees, then the CMRS licensee must provide a point of contact suitable for receiving qualifying requests to disable contraband wireless devices in correctional facilities. With regard to carrier investigations, the Commission seeks comment on a range of possible options, including requiring the carrier to immediately disable the wireless devices upon receipt of a qualifying request from an authorized party without conducing any investigation; requiring the carrier to conduct brief research of readily accessible data prior to disabling or to respond to a series of Commission questions regarding the status of the wireless device to determine its status; or requiring the carrier to use all data at its disposal prior to disabling. The FNPRM seeks comment on all aspects of the disabling process regarding verification of disabling requests, particularly the costs and benefits to the wireless providers, CIS operators, and the correctional facilities.

63. With respect to the appropriate timeframe for disabling a contraband wireless device, or rejecting the request if appropriate, the Commission seeks comment on various options, each of which might be impacted by the range of potential levels of carrier investigation in independently verifying a disabling request and customer outreach. The Commission believes that appropriate timeframes should strike a reasonable balance between the need for prompt action to disable a contraband device potentially used for criminal purposes, and licensee resources required to either verify and implement, or reasonably reject a qualifying request.

64. While the Commission seeks comment on a CIS eligibility process that will substantially ensure that only contraband wireless devices located within correctional facilities are identified for carrier disabling, we also recognize that in limited instances a non-contraband device in close proximity to a correctional facility might be mistakenly identified as contraband and disabled in error. In the event of such an error, the Commission seeks comment on what timely and efficient methods wireless providers can implement to minimize customer inconvenience to resume service to the device.

65. The Commission has considered various alternatives, including a court order process or a voluntary carrier termination process, on which it seeks comment. The Commission sought comment on a proposal seeking adoption of a rule to insulate carriers from any legal liability for wrongful termination. The Commission noted that wireless carriers' current end user licensing agreements may already protect the carriers, but seeks further comment on this proposal, and on whether the Commission should create a safe harbor by rule for wireless providers that comply with the federal process for disabling phones in correctional facilities. The Commission also seeks comment on whether and to what extent a system used to request wireless provider disabling of a contraband wireless device pursuant to a Commission rule raises issues under Title 18 of the U.S. Code or section 705 of the Communications Act, as amended (Act), that may be different from those raised by MAS implementation. The Commission does not find that the record supports the position that section 222 of the Act would prohibit a carrier from complying with a disabling process, but seeks comment on the issue to the extent commenters maintain a contrary view.

66. In the alternative, the Commission seeks comment on additional technological means of combating contraband devices, including imposition of quiet zones around correctional facilities, network-based solutions, and incorporation of beacon technology into wireless handsets that would provide a software method of disabling functionality within correctional facilities

67. Legal Basis. The legal basis for any action that may be taken pursuant to the FNPRM is contained in sections 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332.

68. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted (15 U.S.C. 603(b)(3)). The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction" (5 U.S.C. 601(6)). In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act (5 U.S.C. 601(3)). A small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA (5 U.S.C. 601(3)).

69. Small Businesses, Small Organizations, Small Governmental Jurisdictions. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three comprehensive small entity size standards that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States which translates to 28.8 million businesses. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." Nationwide, as of 2007, there were approximately 1,621,215 small organizations. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau

data published in 2012 indicate that there were 89,476 local governmental jurisdictions in the United States. We estimate that, of this total, as many as 88,761 entities may qualify as "small governmental jurisdictions." Thus, we estimate that most governmental jurisdictions are small.

70. Wired Telecommunications Carriers. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees. U.S. Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees. Thus, under this size standard, the majority of firms in this industry can be considered small.

71. Neither the Commission nor the SBA has developed a definition for Interexchange Carriers. The closest NAICS Code category is Wired Telecommunications Carriers and the applicable small business size standard under SBA rules consists of all such companies having 1,500 or fewer employees. U.S. Census data for 2012 indicates that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees. According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services. Of this total, an estimated 317 have 1,500 or fewer employees. Consequently,

the Commission estimates that the majority of interexchange service providers are small entities that may be affected by the rules adopted.

72. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. Under the SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services. Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

73. Toll Resellers. The SBA has not developed a small business size standard specifically for the category of Toll Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for toll resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this

industry. Under the SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services. Of these, an estimated 857 have 1,500 or fewer employees and 24 have more than 1,500 employees. Consequently, the Commission estimates that the majority of toll resellers are small entities that may be affected by the rules adopted.

74. Other Toll Carriers. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable size standard under SBA rules is for Wired Telecommunications Carriers and the applicable small business size standard under SBA rules consists of all such companies having 1,500 or fewer employees. U.S. Census data for 2012 indicates that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees. According to Commission data, 284 companies reported that their primary telecommunications service activity was the provision of other toll carriage. Of these, an estimated 279 have 1,500 or fewer employees and five have more than 1,500 employees. Consequently, the Commission estimates that most Other Toll Carriers are small entities that may be affected by the rules and policies adopted.

75. 800 and 800-Like Service Subscribers. Neither the Commission nor the SBA has developed a small business size standard specifically for 800 and 800-like service (toll free) subscribers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees. The most reliable source of

information regarding the number of these service subscribers appears to be data the Commission collects on the 800, 888, 877, and 866 numbers in use. According to our data, as of September 2009, the number of 800 numbers assigned was 7,860,000; the number of 888 numbers assigned was 5,588,687; the number of 877 numbers assigned was 4,721,866; and the number of 866 numbers assigned was 7,867,736. We do not have data specifying the number of these subscribers that are not independently owned and operated or have more than 1,500 employees, and thus are unable at this time to estimate with greater precision the number of toll free subscribers that would qualify as small businesses under the SBA size standard. Consequently, we estimate that there are 7,860,000 or fewer small entity 800 subscribers; 5,588,687 or fewer small entity 888 subscribers; 4,721,866 or fewer small entity 877 subscribers; and 7,867,736 or fewer small entity 866 subscribers.

76. Wireless Telecommunications Carriers (except Satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, U.S. Census data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms had employment of 999 or fewer employees and 12 had employment of 1000 employees or more. Thus under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

77. Broadband Personal Communications Service. The broadband personal communications service (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission defined "small entity" for Blocks C and F as an entity that has average gross revenues of $40 million or less in the three previous calendar years. For Block F, an

additional classification for “very small business” was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years. These standards defining “small entity” in the context of broadband PCS auctions have been approved by the SBA. No small businesses, within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that qualified as small entities in the Block C auctions. A total of 93 small and very small business bidders won approximately 40 percent of the 1,479 licenses for Blocks D, E, and F. In 1999, the Commission re-auctioned 347 C, E, and F Block licenses. There were 48 small business winning bidders. In 2001, the Commission completed the auction of 422 C and F Broadband PCS licenses in Auction 35. Of the 35 winning bidders in this auction, 29 qualified as “small” or “very small” businesses. Subsequent events, concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. In 2005, the Commission completed an auction of 188 C block licenses and 21 F block licenses in Auction 58. There were 24 winning bidders for 217 licenses. Of the 24 winning bidders, 16 claimed small business status and won 156 licenses. In 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction 71. Of the 14 winning bidders, six were designated entities. In 2008, the Commission completed an auction of 20 Broadband PCS licenses in the C, D, E and F block licenses in Auction 78.

78. Advanced Wireless Services. AWS Services (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3)). For the AWS-1 bands, the Commission has defined a “small business” as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a “very small business” as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for

cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.

79. Specialized Mobile Radio. The Commission awards small business bidding credits in auctions for Specialized Mobile Radio ("SMR") geographic area licenses in the 800 MHz and 900 MHz bands to entities that had revenues of no more than $15 million in each of the three previous calendar years. The Commission awards very small business bidding credits to entities that had revenues of no more than $3 million in each of the three previous calendar years. The SBA has approved these small business size standards for the 800 MHz and 900 MHz SMR Services. The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz bands. The 900 MHz SMR auction was completed in 1996. Sixty bidders claiming that they qualified as small businesses under the $15 million size standard won 263 geographic area licenses in the 900 MHz SMR band. The 800 MHz SMR auction for the upper 200 channels was conducted in 1997. Ten bidders claiming that they qualified as small businesses under the $15 million size standard won 38 geographic area licenses for the upper 200 channels in the 800 MHz SMR band. A second auction for the 800 MHz band was conducted in 2002 and included 23 BEA licenses. One bidder claiming small business status won five licenses.

80. The auction of the 1,053 800 MHz SMR geographic area licenses for the General Category channels was conducted in 2000. Eleven bidders won 108 geographic area licenses for the General Category channels in the 800 MHz SMR band qualified as small businesses under the $15 million size standard. In an auction completed in 2000, a total of 2,800 Economic Area licenses in the lower 80 channels of the 800 MHz SMR service were awarded. Of the 22 winning bidders, 19 claimed small

business status and won 129 licenses. Thus, combining all three auctions, 40 winning bidders for geographic licenses in the 800 MHz SMR band claimed status as small business.

81. In addition, there are numerous incumbent site-by-site SMR licensees and licensees with extended implementation authorizations in the 800 and 900 MHz bands. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. In addition, we do not know how many of these firms have 1500 or fewer employees. We assume, for purposes of this analysis, that all of the remaining existing extended implementation authorizations are held by small entities, as that small business size standard is approved by the SBA.

82. Lower 700 MHz Band Licenses. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits. The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years. A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years. The SBA approved these small size standards. An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of

329 licenses. A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses. Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses. On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

83. In 2007, the Commission reexamined its rules governing the 700 MHz band. An auction of 700 MHz licenses commenced January 24, 2008 and closed on March 18, 2008, which included, 176 Economic Area licenses in the A Block, 734 Cellular Market Area licenses in the B Block, and 176 EA licenses in the E Block. Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

84. Upper 700 MHz Band Licenses. On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block. The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

85. Satellite Telecommunications. This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling

satellite telecommunications." The category has a small business size standard of $32.5 million or less in average annual receipts, under SBA rules. For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year. Of this total, 299 firms had annual receipts of less than $25 million. Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

86. All Other Telecommunications. The "All Other Telecommunications" category is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry. The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less. For this category, U.S. Census data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million. Thus, a majority of "All Other Telecommunications" firms potentially affected by the rules adopted can be considered small.

87. Other Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment). Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing. The SBA has established a size standard for this industry as 750 employees or less. Census data for 2012 show that

383 establishments operated in that year. Of that number, 379 operated with less than 500 employees. Based on that data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

88. Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment. The SBA has established a size standard for this industry of 750 employees or less. U.S. Census data for 2012 show that 841 establishments operated in this industry in that year. Of that number, 819 establishments operated with less than 500 employees. Based on this data, we conclude that a majority of manufacturers in this industry is small.

89. Engineering Services. This industry comprises establishments primarily engaged in applying physical laws and principles of engineering in the design, development, and utilization of machines, materials, instruments, structures, process, and systems. The assignments undertaken by these establishments may involve any of the following activities: provision of advice, preparation of feasibility studies, preparation of preliminary and final plans and designs, provision of technical services during the construction or installation phase, inspection and evaluation of engineering projects, and related services. The SBA deems engineering services firms to be small if they have $15 million or less in annual receipts, except military and aerospace equipment and military weapons engineering establishments are deemed small if they have $38 million or less an annual receipts. According to U.S. Census Bureau data for 2012, there were 49,092 establishments in this category that operated the full year. Of the 49,092 establishments, 45,848 had less than $10 million in receipts and 3,244 had $10 million or more in annual receipts. Accordingly, the Commission estimates that a majority of engineering service firms are small.

90. Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System Instrument Manufacturing. This U.S. industry comprises establishments primarily engaged in manufacturing search, detection, navigation, guidance, aeronautical, and nautical systems and instruments. Examples of products made by these establishments are aircraft instruments (except engine), flight recorders, navigational instruments and systems, radar systems and equipment, and sonar systems and equipment. The SBA has established a size standard for this industry of 1,250 employees or less. Data from the 2012 Economic Census show 588 establishments operated during that year. Of that number, 533 establishments operated with less than 500 employees. Based on this data, we conclude that the majority of manufacturers in this industry are small.

91. Security Guards and Patrol Services. The U.S. Census Bureau defines this category to include "establishments primarily engaged in providing guard and patrol services." The SBA deems security guards and patrol services firms to be small if they have $18.5 million or less in annual receipts. According to U.S. Census Bureau data for 2012, there were 8,742 establishments in operation the full year. Of the 8,842 establishments, 8,276 had less than $10 million while 466 had more than $10 million in annual receipts. Accordingly, the Commission estimates that a majority of firms in this category are small.

92. All Other Support Services. This U.S. industry comprises establishments primarily engaged in providing day-to-day business and other organizational support services (except office administrative services, facilities support services, employment services, business support services, travel arrangement and reservation services, security and investigation services, services to buildings and other structures, packaging and labeling services, and convention and trade show organizing services). The SBA deems all other support services firms to be small if they have $11 million or less in annual receipts. According to U.S. Census Bureau data for 2012, there were 11,178 establishments in operation the full year. Of the 11,178 establishments, 10,886 had less than $10 million while 292 had greater than $10 million in

annual receipts. Accordingly, the Commission estimates that a majority of firms in this category are small.

93. Correctional Institutions (State and Federal Facilities). This industry comprises government establishments primarily engaged in managing and operating correctional institutions. The Department of Justice's Bureau of Justice Statistics (BJS) collects and publishes census information on adult correctional facilities operating under state or federal authority as well as private and local facilities operating under contract to house inmates for federal or state correctional authorities. The types of facilities included in the census data from BJS are prisons and prison farms; prison hospitals; centers for medical treatment and psychiatric confinement; boot camps; centers for reception; diagnosis; classification; alcohol and drug treatment; community correctional facilities; facilities for parole violators and other persons returned to custody; institutions for youthful offenders; and institutions for geriatric inmates.

94. While neither the SBA nor the Commission have developed a size standard for this category, the size standard for a small facility in the BJS census data is one that has an average daily population (ADP) of less than 500 inmates. The latest BJS census data available shows that as of December 30, 2005 there were a total of 1821 correctional facilities operating under state or local federal authority. Of that number more than half of the facilities or a total 946 facilities had an average daily population of less than 500 inmates. Based on this data a majority of "Governmental Correctional Institutions" potentially affected by the rules adopted can be considered small.

95. Facilities Support Services. This industry comprises establishments primarily engaged in providing operating staff to perform a combination of support services within a client's facilities. Establishments providing facilities (except computer and/or data processing) operation support services and establishments providing private jail services or operating correctional facilities (i.e., jails) on a

contract or fee basis are included in this industry. Establishments in this industry typically provide a combination of services, such as janitorial, maintenance, trash disposal, guard and security, mail routing, reception, laundry, and related services to support operations within facilities. These establishments provide operating staff to carry out these support activities, but are not involved with or responsible for the core business or activities of the client. The SBA has developed a small business size standard for "Facilities Support Services," which consists of all such firms with gross annual receipts of $38.5 million or less. For this category, U.S. Census data for 2012 shows that there were 5,344 firms that operated for the entire year. Of these firms, 4,882 had gross annual receipts of less than $10 million and 462 had gross annual receipts of $10 million or more. Based on this data a majority of "Facilities Support Services" firms potentially affected by the rules adopted can be considered small.

96. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities. In the FNPRM, the Commission seeks public comment on methods to improve the viability of technologies used to combat contraband wireless devices in correctional facilities. The potential process is prospective in that it would only apply if an entity avails itself of managed access or detection technologies. There are three classes of small entities that might be impacted: providers of wireless services, providers or operators of managed access or detection systems, and correctional facilities.

97. For small entities that are providers of wireless services and enter into lease arrangements with CIS operators, the Commission seeks notice on a requirement that those entities provide advanced notice prior to certain changes in the CMRS licensee's network. We seek comment on limiting the notice requirement to particular changes in the carrier's network – e.g., additions of new frequency bands – in order to ensure the notice requirement does not result in an unnecessary burden on CMRS licensees, but seek comment on what other notice requirements might be necessary to ensure effective CIS operation. The FNPRM also seeks comment on a process whereby CMRS providers would disable

contraband wireless devices detected within a correctional facility upon receipt of a qualifying request. In order to receive qualifying requests, the FNPRM seeks comment on a requirement that CMRS licensees who enter into lease arrangements with CIS operators to have a verifiable transmittal mechanism in place and, upon request, provide a DCFO with a point of contact suitable for receiving qualifying requests. We note that some carriers may already have such secure portals in place for receipt of similar requests. The costs of complying with a disabling process would vary depending on the level of investigation required of carriers upon receiving a qualifying request. The Commission seeks comment on this issue, but notes that several carriers already have internal procedures for disabling contraband wireless devices pursuant to court orders, which could be modified to accommodate a disabling process. Nevertheless, these requirements would likely require the allocation of resources to tailor internal processes, including some level of additional staffing.

98. The FNPRM also contemplates the option of requiring CMRS licensees to perform varying levels of customer outreach upon receiving a qualifying request, or after disabling a contraband wireless device. The Commission seeks comment on the costs and benefits of this proposal, but notes carriers may already have mechanisms in place for customer outreach.

99. The Commission seeks to streamline the process for identification, notification, and disabling of contraband devices to the greatest extent possible, while also ensuring the accuracy, security, and efficiency of such a process. Therefore, the FNPRM seeks comment on a process that would require small entity CIS operators, as well as all other CIS operators, to be deemed eligible and provide various pieces of required information along with a qualifying request for disabling a contraband device to the wireless carriers. Specifically, in order to be eligible, the Commission asks whether a CIS operator should demonstrate the following: (1) the CIS has appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility, secure and protect the collected information, and avoid interfering with emergency

911 calls; and (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to provide a high degree of certainty that the particular wireless device is in fact located within a correctional facility.

100. The Commission seeks comment on an eligibility process that would apply equally to all CIS operators, irrespective of size. We note that a mandatory process for disabling contraband wireless devices identified using detection systems does not currently exist, and, without adoption of a process like that considered in the FNPRM, is subject to the discretion of wireless carriers to voluntarily disable devices. It is possible that an outgrowth of the questions asked and responses received could result in additional requirements for being deemed an eligible CIS, submitting qualifying requests, and disabling contraband devices. This may also require some level of recordkeeping to ensure that contraband wireless devices, and not legitimate devices, are disabled. To the extent the process would impose these requirements, they would be necessary to ensure that legitimate wireless users are not impacted by the operation of CISs, which should be the minimum performance objective for any detection system. Therefore, while these requirements might impose some compliance or recordkeeping obligations, they would be a necessary predicate for the operation of a detection system

101. In the FNPRM, we also seek comment on requiring correctional facilities wishing to use CIS as a means of combatting contraband cellphones use inside the prison to designate a DCFO. The Commission seeks comment on whether qualifying requests should be transmitted either by the Commission upon the request of the DCFO, or by the DCFO. If the DCFO is to transmit the requests, the Commission also seeks comment on a requirement that the DCFO certify in the qualifying request that: (1) an eligible CIS was used in the correctional facility, and include evidence of such eligibility; (2) the CIS is authorized for operation through a license or Commission approved lease agreement, referencing the applicable ULS identifying information; (3) the DCFO has contacted all CMRS licensees providing service in the area of the correctional facility for which it will seek device disabling in order to establish a

verifiable transmission mechanism for making qualifying requests and for receiving notifications from the licensee; and (4) it has substantial evidence that the contraband wireless device was used in the correctional facility, and that such use was observed within the 30 day period immediately prior to the date of submitting the request. It is possible that an outgrowth of the questions asked and responses received could result in additional reporting and recordkeeping requirements on the DCFO and its respective correctional facility. The goal of imposing such requirements on the DCFO, however, would be to provide an efficient means of communication among CIS operators, correctional facilities, and CMRS providers, and to ensure the accuracy and legitimacy of any termination process

102. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof for small entities."

103. First, in the FNPRM, the Commission contemplates the possibility that the obligations considered might create additional compliance costs on CMRS licensees and CIS operators, both large and small. However, the Commission seeks comment on the specific criteria and timetables that should be required, and the associated costs and benefits in order to facilitate informed decisions in the final rules. Specifically, the Commission considers a range of timeframes in which CMRS licensees would be required to respond to qualifying requests and seeks comment on the resource and staff demands associated with those timeframes. With respect to the demands on CIS operators, the FNPRM considers a range of certifications and necessary information to be included with qualifying requests, and seeks

comment on which pieces of information are important to accurately identify contraband wireless devices. Commenters are asked whether small entities face any special or unique issues with respect to terminating service to devices, and whether they would require additional time to take such action. In doing so, the Commission seeks to ensure the accuracy, security, and efficiency of the identification and disabling process, while also minimizing compliance burdens to the greatest extent possible

104. Second, to limit the economic impact of a notice requirement, we seek comment on the types of network changes that should require advanced notification to CIS providers. While the Commission emphasizes the importance of cooperation between CIS operators and CMRS providers at every stage of CIS deployment, we also recognize the potential for overly burdensome notice requirements that would require notice upon making any network changes, even those that are unlikely to negatively impact the CIS.

105. Third, in order to clarify and simplify compliance and reporting requirements for small entities, as well as all other impacted entities, the Commission intends to designate a single point of contact at the Commission to serve as the ombudsperson on contraband wireless device issues. The ombudsperson's duties may include, as necessary, providing assistance to CIS operators in connecting with CMRS licensees, playing a role in identifying required CIS filings for a given correctional facility, facilitating the required Commission filings, thereby reducing regulatory burdens, and resolving issues that may arise during the leasing process. The ombudsperson will also conduct outreach and maintain a dialogue with all stakeholders on the issues important to furthering a solution to the problem of contraband wireless device use in correctional facilities. Finally, the ombudsperson, in conjunction with WTB, will maintain webpage with a list of active CIS operators and locations where CIS has been deployed. The appointment of an ombudsperson provides an important resource for small entities to understand and comply with any CIS-related requirements.

106. While the FNPRM considers a requirement that CISs be deemed eligible prior to making a qualifying request, the Commission does not seek comment on any specific design standard. Instead, the Commission seeks comment on the elements of detection systems and identification methods that contribute to the accuracy and reliability of a particular CIS. The FNPRM asks whether the standard should differ between rural and urban areas, or between large and small detection system providers or operators.

107. Finally, the FNPRM does not propose any exemption for small entities. The Commission finds an overriding public interest in preventing the illicit use of contraband wireless devices by prisoners to perpetuate criminal enterprises. The CIS eligibility requirement discussed in the FNPRM would be vital to the accuracy and reliability of the information ultimately used to disable contraband wireless devices, regardless of the size of the entity obtaining that information. Further, to the extent that a small entity could be exempt from a disabling requirement, it would reduce the overall effectiveness of a CIS. If inmates discover that a wireless provider whose service area includes the correctional facility does not disable contraband wireless devices within the facility, inmates will accordingly use only that service. Therefore, while the Further Notice seeks comment on alternative considerations for the overall identification and disabling process to accommodate the needs and resources of small entities, an exemption would be contrary to the Commission's overarching goal of combatting contraband wireless devices in wireless facilities.

108. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules. The FNPRM seeks comment on the application and relevance of sections 705 and 222 of the Act and Title 18 of the U.S. Code.

Congressional Review Act

109. The Commission will send a copy of the FNPRM to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

III. ORDERING CLAUSES

110. IT IS ORDERED that, pursuant to the authority contained in sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332, the FNPRM in GN Docket No. 13-111 IS ADOPTED.

111. IT IS FURTHER ORDERED that, pursuant to applicable procedures set forth in sections 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments on the FNPRM on or before 30 days after publication in the Federal Register and reply comments on or before 60 days after publication in the Federal Register.

112. IT IS FURTHER ORDERED that, pursuant to section 801(a)(1)(A) of the Congressional Review Act, 5 U.S.C. 801(a)(1)(A), the Commission SHALL SEND a copy of the FNPRM to Congress and to the Government Accountability Office.

113. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of the FNPRM, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 20

Communications common carriers, Radio

FEDERAL COMMUNICATIONS COMMISSION.

Marlene H. Dortch,
Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to further amend 47 CFR part 20, as amended in a final rule published elsewhere in this issue of the Federal Register, as set forth below:

PART 20—Commercial Mobile Radio Services

1. The authority citation for part 20 continues to read as follows:

AUTHORITY: 47 U.S.C. 151, 152(a), 154(i), 157, 160, 201, 214, 222, 251(e), 301, 302, 303, 303(b), 303(r), 307, 307(a), 309, 309(j)(3), 316, 316(a), 332, 610, 615, 615a, 615b, 615c, unless otherwise noted.

2. Amend § 20.23 by adding paragraph (b) to read as follows**:**

§ 20.23 Contraband wireless devices in correctional facilities.

* * * * *

(b) Disabling contraband wireless devices. A Designated Correctional Facility Official may request that a CMRS licensee disable a contraband wireless device in a correctional facility detected by a Contraband Interdiction System as described below.

(1) Licensee obligation. A licensee providing CMRS service must:

(i) Upon request of a Designated Correctional Facility Official, provide a point of contact suitable for receiving qualifying requests to disable devices; and

(ii) Upon request of a Designated Correctional Facility Office to disable a contraband wireless devices, verify that the request is a qualifying request and, if so, permanently disable the device.

(2) Qualifying request. A qualifying request must be made in writing via a verifiable transmission mechanism, contain the certifications in paragraph (3) of this section and the device and correctional facility identifying information in paragraph (4) of this section, and be signed by a Designated Correctional Facility Official. For purposes of this section, a Designated

Correctional Facility Official means a state or local official responsible for the correctional facility where the contraband device is located.

(3) Certifications. A qualifying request must include the following certifications by the Designated Correctional Facility Official:

(i) The CIS used to identify the device is authorized for operation through a Commission license or approved lease agreement, referencing the applicable ULS identifying information;

(ii) The Designated Correctional Facility Official has contacted all CMRS licensees providing service in the area of the correctional facility in order to establish a verifiable transmission mechanism for making qualifying requests and for receiving notifications from the CMRS licensee;

(iii) The Designated Correctional Facility Official has substantial evidence that the contraband wireless device was used in the correctional facility, and that such use was observed within the 30 day period immediately prior to the date of submitting the request; and

(iv) The CIS used to identify the device is an Eligible CIS as defined in paragraph (5) of this section. The Designated Correctional Facility Official must include a copy of a FCC Public Notice listing the eligible CIS.

(4) Device and correctional facility identifying information. The request must identify the device to be disabled and correctional facility by providing the following information:

(i) Identifiers sufficient to uniquely describe the device in question;

(ii) Licensee providing CMRS service to the device;

(iii) Name of correctional facility;

(iv) Street address of correctional facility;

(v) Latitude and longitude coordinates sufficient to describe the boundaries of the correctional facility; and

(vi) Call signs of FCC Licenses and/or Leases authorizing the CIS.

(5) Eligible CIS. (i) In order to be listed on a FCC Public Notice as an Eligible CIS, a CIS operator must demonstrate to the Commission that:

(A) All radio transmitters used as part of the CIS have appropriate equipment authorization pursuant to Commission rules;

(B) The CIS is designed and will be configured to locate devices solely within a correctional facility, secure and protect the collected information, and is capable of being programmed not to interfere with emergency 911 calls; and

(C) The methodology to be used in analyzing data collected by the CIS is sufficiently robust to provide a high degree of certainty that the particular wireless device is in fact located within a correctional facility.

(ii) Periodically, the Commission will issue Public Notices listing all Eligible CISs.

[FR Doc. 2017-09886 Filed: 5/17/2017 8:45 am; Publication Date: 5/18/2017]